

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

1. - 44. (cancelled)

45. (currently amended) A computer implemented method for server-side execution in support of financial transactions, comprising:

establishing an authentication record at the in memory accessible by server-side computer resources, in response to communications at a first time from a particular account holder, for a predicted transaction by [[a]] the particular account holder, the authentication record for the predicted transaction includes having a predicted transaction amount, and a transaction time parameter, and an authenticated transaction signature for presentation upon execution of the predicted transaction, and sending a message including the authenticated transaction signature from the server-side computer resources to the particular account holder;

establishing an authorization record in memory accessible by server-side computer resources, in response to communications at a second time from a party to a particular transaction, for [[a]] the particular transaction indicating an actual transaction amount, an actual transaction time and a presented transaction signature, wherein said establishing an authorization record does not require identification of the particular account holder;

reading and processing the authorization record and the authentication record in the server-side computer resources, and if determining whether the presented transaction signature in the authorization record matches the authenticated transaction signature in the authentication record for the predicted transaction, the actual transaction amount in the authorization record matches the predicted transaction amount in the authentication record and the actual transaction time in the authorization record matches the transaction time parameter in the authentication record, then sending an authorization message to the party of the particular transaction; and

reconciling the predicted transaction amount and the actual transaction amount in the server-side computer resources, for the particular account holder.

46. (original) The method of claim 45, including:

2 storing the authentication record in a database including a plurality of authentication
3 records for other predicted transactions.

1 47. (currently amended) The method of claim 45, wherein the time parameter comprises a time
2 value ~~indicated~~ indicating the first time, when the authorization record was created.

1 48. (original) The method of claim 45, wherein said matching includes determining whether the
2 actual transaction time falls within a time interval indicated by the transaction time parameter.

1 49. (previously presented) The method of claim 45, wherein establishing an authentication record
2 includes:

3 establishing a communication session with the particular account holder;
4 accepting an account number and an identification number for the particular account
5 holder via the communication session;
6 accepting the predicted transaction amount via the communication session; and
7 producing the transaction signature.

1 50. (original) The method of claim 49, including prompting the particular account holder to
2 supply a combination of digits from a personal identification code, wherein the combination does
3 not include all of the personal identification code.

1 51. (currently amended) The method of claim 45, wherein establishing an authorization record
2 includes:

3 establishing a communication session with ~~[[a]]~~ the party to the particular transaction;
4 and
5 accepting the presented transaction signature and the actual transaction amount via the
6 communication session.

1 52. (previously presented) The method of claim 51, including accepting identification of the
2 party via the communication session.

1 53. (previously presented) The method of claim 52, including maintaining a list of authorized
2 parties, and including determining whether the identification of the party accepted via the
3 communication session indicates a party in the list of authorized parties.

1 54. (cancelled)

1 55. (previously presented) The method of claim 45, wherein establishing an authentication record
2 includes:

3 establishing a communication session with the particular account holder;

4 accepting an account number via the communication session;

5 prompting the particular account holder via the communication session to supply a static
6 identification number and a dynamically identified combination of digits from a personal
7 identification code, wherein the combination does not include all of the personal identification
8 code;

9 accepting the predicted transaction amount via the communication session; and

10 producing the transaction signature and sending the transaction signature to the particular
11 account holder.

1 56. - 57. (cancelled)

1 58. (new) A method for managing financial transactions using a computer system arranged
2 for communication with remote devices using communication lines, comprising:

3 performing a plurality of authentication processes in response to initiations of respective
4 sessions with the computer system by data communications from remote devices, for predicted
5 transactions having predicted transaction amounts and predicted transaction time out intervals by
6 particular account holders, the authentication processes respectively characterized by the steps of

7 generating in the computer system requests for input for the corresponding

8 predicted transaction, and receiving in the computer responses to the

9 requests for input from one of said remote devices, wherein said

10 responses to the requests include an identifier of the account used for

11 authenticating the account, at least one factor unique to the account

12 holder for authenticating the account holder and at least two factors

13 related to the predicted transaction including a transaction specific
14 factor and a transaction type identifier unique to the account holder
15 used for authenticating the predicted transaction;
16 storing a first time-stamped record in memory including the identifier of the
17 account, the at least one factor unique to the account holder, the
18 transaction specific factor, the transaction type identifier and a time
19 parameter as a part of or as data associated with the first record in
20 memory; and
21 producing a transaction signature as a function of the identifier of the account,
22 the at least one factor unique to the account holder, the transaction
23 specific factor, the transaction type identifier and the time parameter,
24 for presentation upon execution of the predicted transaction upon
25 authenticating the account, the account holder and the predicted
26 transaction using said responses, associating the transaction signature
27 with the first time-stamped record and transmitting the transaction
28 signature to one of said remote devices associated with the particular
29 account holder;
30 performing, in the computer system, a plurality of authorization processes for particular
31 transactions in response to authorization requests from parties to actual transactions, the
32 authorization process for a particular transaction characterized by the steps of
33 receiving an account identifier, a presented transaction signature, and an actual
34 transaction amount at an actual transaction time associated with the
35 authorization request for the particular transaction having a transaction
36 type from one of said remote devices;
37 storing a second time-stamped record in memory for the authorization request
38 for the particular transaction, the record including the received account
39 identifier, the presented transaction signature, the actual transaction
40 amount and the actual transaction time;
41 processing the second time-stamped record, in response to one of said first
42 time-stamped records with a matching account identifier, to verify that
43 the presented transaction signature matches the transaction signature
44 associated with said one of said first records, the actual transaction

45 amount matches the predicted transaction amount associated with said
46 one of said first time-stamped records, the actual transaction type
47 matches the transaction type associated with said one of said first
48 records and the actual transaction time is within the predicted
49 transaction time out interval; and
50 transmitting authorization signals upon successful authorization to one of said
51 remote devices associated with said particular transaction; and
52 performing, in the computer system, a plurality of accounting processes for respective
53 transactions subject of authorization processes, including reconciling the predicted transaction
54 amounts and the actual transaction amounts for each transaction of the particular account
55 holders.

1 59. (new) The method of claim 58, including:
2 storing the predicted transaction type identifier, the predicted transaction amount, and the
3 transaction signature for a predicted transaction in a database in said memory.

1 60. (new) The method of claim 58, including storing a predicted transaction time out
2 interval parameter in the database.

1 61. (new) The method of claim 58, including setting up a time out interval between the
2 authentication process and the authorization process and after creation of a first time-stamped
3 record for a particular account, monitoring the memory to detect creation of a second time-
4 stamped record having a matching account identifier and attempting said authorization process
5 until one of expiration of the time out interval and success of the authorization process.

1 62. (new) The method of claim 58, wherein the authentication process is further
2 characterized by executing a process in the computer system prompting the particular account
3 holder via the communication lines to supply to the computer system a transaction specific code
4 based on or equal to a combination of alphanumeric characters at certain randomly chosen
5 alphanumeric character positions in a password, wherein the combination does not include all of
6 the alphanumeric characters in the password.

1 63. (new) The method of claim 58, wherein the authorization process includes:
2 at the server, performing a plurality of authorization processes for particular transactions
3 in response to authorization requests from parties to actual transactions characterized by
4 prioritizing pairs of first time-stamped records and second time-stamped records with matching
5 account identifiers according to their time stamps and time out interval parameters.

1 64. (new) The method of claim 58, including accepting identification of the party at the
2 server.

1 65. (new) The method of claim 58, wherein the authorization process operates without
2 identification of the particular account holder to the party.

1 66. (new) The method of claim 58, wherein the authorization process operates with
2 identification of the particular account holder to the party.

1 67. (new) A financial transaction server, comprising:
2 a communication interface;
3 a computer system including memory coupled to the communication interface, the data
4 processing system including resources for managing financial transactions and for
5 communicating using the communication interface with remote devices, including
6 an authentication process communicating over the communication interface for
7 authenticating predicted transaction by a particular account holder, including routines
8 characterized by the steps of
9 generating in the computer system requests for input for the corresponding
10 predicted transaction, and receiving in the computer responses to the
11 requests for input from one of said remote devices, wherein said
12 responses to the requests include an identifier of the account used for
13 authenticating the account, at least one factor unique to the account
14 holder for authenticating the account holder and at least two factors
15 related to the predicted transaction including a transaction specific
16 factor and a transaction type identifier unique to the account holder
17 used for authenticating the predicted transaction;

18 storing a first time-stamped record in memory including the identifier of the
19 account, at least one factor unique to the account holder for
20 authenticating the account holder, the transaction specific factor, the
21 transaction type identifier and a time parameter as a part of or as data
22 associated with the first record in memory; and
23 producing a transaction signature as a function of the identifier of the account,
24 the at least one factor unique to the account holder, the transaction
25 specific factor, the transaction type identifier and the time parameter,
26 for presentation upon execution of the predicted transaction upon
27 authenticating the account, the account holder and the predicted
28 transaction using said responses, associating the transaction signature
29 with the first time-stamped record and transmitting the transaction
30 signature to one of said remote devices associated with the particular
31 account holder;

32 an authorization process communicating over the communication interface for
33 authorizing a particular transaction having actual transaction amount and an actual transaction
34 time, including routines characterized by the steps of
35 receiving an account identifier, a presented transaction signature, and an actual
36 transaction amount at an actual transaction time associated with the
37 authorization request for the particular transaction having a transaction
38 type from one of said remote devices;

39 storing a second time-stamped record in memory for the authorization request
40 for the particular transaction, the record including the received account
41 identifier, the presented transaction signature, the actual transaction
42 amount and the actual transaction time;

43 processing the second time-stamped record, in response to one of said first
44 time-stamped records with a matching account identifier, to verify that
45 the presented transaction signature matches the transaction signature
46 associated with said one of said first records, the actual transaction
47 amount matches the predicted transaction amount associated with said
48 one of said first time-stamped records, the actual transaction type
49 matches the transaction type associated with said one of said first

50 records and the actual transaction time is within the predicted
51 transaction time out interval; and
52 transmitting authorization signals upon successful authorization to one of said
53 remote devices associated with said particular transaction; and
54 an accounting process executed in combination with said authorization processes for
55 respective transactions, including reconciling the predicted transaction amounts and the actual
56 transaction amounts for each transaction of the particular account holders.

1 68. (new) The financial transaction server of claim 67, wherein the data processing system
2 includes a local or remote database storing the first and second time-stamped records.

1 69. (new) The financial transaction server of claim 67, wherein the data processing system
2 includes a watchdog routine which after creation of a first time-stamped record for a particular
3 account, monitors the memory to detect creation of a second time-stamped record having a
4 matching account identifier and attempts said authorization process until one of expiration of the
5 time out interval and success of the authorization process.

1 70. (new) The financial transaction server of claim 67, wherein the authentication process
2 includes routines performing a plurality of authorization processes for particular transactions in
3 response to authorization requests from parties to actual transactions characterized by prioritizing
4 pairs of first time-stamped records and second time-stamped records with matching account
5 identifiers according to their time stamps and time out interval parameters.

1 71. (new) The financial transaction server of claim 67, wherein the authentication process
2 includes a routine prompting the particular account holder via the communication interface to
3 supply to the computer system a transaction specific code based on or equal to a combination of
4 alphanumeric characters at certain randomly chosen alphanumeric character positions in a
5 password, wherein the combination does not include all of the alphanumeric characters in the
6 password.

1 72. (new) The financial transaction server of claim 67, wherein the authorization process
2 includes a routine accepting identification of the party at the server.

1 73. (new) The financial transaction server of claim 67, wherein the authorization process
2 operates without identification of the particular account holder to the party.

1 74. (new) The financial transaction server of claim 67, wherein the authorization process
2 operates with identification of the particular account holder to the party.

1 75. (new) An article of manufacture, comprising:
2 a machine readable storage medium;
3 a computer program stored on said machine readable medium with resources executable
4 by a computer system for managing financial transactions, including
5 an authentication process communicating over the communication interface for
6 authenticating predicted transaction by a particular account holder, including routines
7 characterized by the steps of

8 generating in the computer system requests for input for the corresponding
9 predicted transaction, and receiving in the computer responses to the
10 requests for input from one of said remote devices, wherein said
11 responses to the requests include an identifier of the account used for
12 authenticating the account, at least one factor unique to the account
13 holder for authenticating the account holder and at least two factors
14 related to the predicted transaction including a transaction specific
15 factor and a transaction type identifier unique to the account holder
16 used for authenticating the predicted transaction;

17 storing a first time-stamped record in memory including the identifier of the
18 account, at least one factor unique to the account holder for
19 authenticating the account holder, the transaction specific factor, the
20 transaction type identifier and a time parameter as a part of or as data
21 associated with the first record in memory; and

22 producing a transaction signature as a function of the identifier of the account,
23 the at least one factor unique to the account holder, the transaction
24 specific factor, the transaction type identifier and the time parameter,
25 for presentation upon execution of the predicted transaction upon
26 authenticating the account, the account holder and the predicted

27 transaction using said responses, associating the transaction signature
28 with the first time-stamped record and transmitting the transaction
29 signature to one of said remote devices associated with the particular
30 account holder;

31 an authorization process communicating over the communication interface for
32 authorizing a particular transaction having actual transaction amount and an actual transaction
33 time, including routines characterized by the steps of

34 receiving an account identifier, a presented transaction signature, and an actual
35 transaction amount at an actual transaction time associated with the
36 authorization request for the particular transaction having a transaction
37 type from one of said remote devices;

38 storing a second time-stamped record in memory for the authorization request
39 for the particular transaction, the record including the received account
40 identifier, the presented transaction signature, the actual transaction
41 amount and the actual transaction time;

42 processing the second time-stamped record, in response to one of said first
43 time-stamped records with a matching account identifier, to verify that
44 the presented transaction signature matches the transaction signature
45 associated with said one of said first records, the actual transaction
46 amount matches the predicted transaction amount associated with said
47 one of said first time-stamped records, the actual transaction type
48 matches the transaction type associated with said one of said first
49 records and the actual transaction time is within the predicted
50 transaction time out interval; and

51 transmitting authorization signals upon successful authorization to one of said
52 remote devices associated with said particular transaction; and

53 an accounting process executed in combination with said authorization processes for
54 respective transactions, including reconciling the predicted transaction amounts and the actual
55 transaction amounts for each transaction of the particular account holders.

1 76. (new) The article of claim 75, wherein the resources include a routine for storing the
2 first and second time-stamped records in a local or remote database.

1 77. (new) The article of claim 75, wherein the resources include a watchdog routine which
2 after creation of a first record for a particular account, monitors the memory to detect creation of
3 a second record having a matching account identifier and attempts said authorization process
4 until one of expiration of the time out interval and success of the authorization process.

1 78. (new) The article of claim 75, wherein the authentication process includes a routine
2 prompting the particular account holder via the communication interface to supply to the
3 computer system a transaction specific code based on or equal to a combination of alphanumeric
4 characters at certain randomly chosen alphanumeric character positions in a password, wherein
5 the combination does not include all of the alphanumeric characters in the password.

1 79. (new) The article of claim 75, wherein the authorization process includes routines
2 performing a plurality of authorization processes for particular transactions in response to
3 authorization requests from parties to actual transactions characterized by prioritizing pairs of
4 first time-stamped records and second time-stamped records with matching account identifiers
5 according to their time stamps and time out interval parameters

1 80. (new) The article of claim 75, wherein the authorization process includes a routine
2 accepting identification of the party at the server.

1 81. (new) The article of claim 75, wherein the authorization process operates without
2 identification of the particular account holder to the party.

1 82. (new) The article of claim 75, wherein the authorization process operates with
2 identification of the particular account holder to the party.